CHAPTER 2

SECURITY PLANNING

0200. GENERAL

a. Each Navy activity/installation will develop and publish a physical security and loss prevention plan, in consonance with regional commanders and their security coordinators.

b. Tenant commands will develop and maintain a physical security plan for their activities that takes into account the host command's physical security plan. These plans will be coordinated with the host command security officer.

c. Security plans for tenant activities on a Navy installation will be integrated into the installation physical security plan. Tenant commands will comply with host activity physical security requirements. These integrated plans will incorporate requirements, policies, and procedures for facilities, equipment, regular and auxiliary security forces, employee training/education, and other elements of security essential to force protection and objectives set forth here.

d. Security planning will be integrated with terrorism threat assessment planning and terrorist incident response planning.

e. Tenant and host commands, as appropriate, will ensure that tenant/host and intra or inter-service support agreements outline complete and detailed physical security requirement responsibilities.

f. Where appropriate and feasible, similar integration and coordination of security planning and implementing of specific measures will be accomplished among Navy activities on a regional basis, and with local law enforcement/host nation security forces.

0201. PHYSICAL SECURITY PLAN CONTENT. The content of the plan is more important than its format. The format should be one that facilitates rather than hinders use of the plan. Higher echelons in the chain of command may prescribe for their subordinates a format that facilitates integration into the next higher echelon's plan.

a. The plan must be a "users" instruction clearly delineating how the command conducts day-to-day security and how it responds to security incidents. It should reflect the detailed implementation of the policy in this manual at the activity and installation level (and regional level, if appropriate and feasible).

b. It will cover all phases of the security operations of the activity/installation. It must also be current and reflect the routine needs of the command as well as unusual situations that require special security considerations/measures.

c. It will provide instruction relative to individual security responsibilities, authority, and procedures for handling and reporting incidents.

d. It will also establish systems for alerting and evacuation of personnel. A set of recognizable alarms should be developed for potential emergencies, each with their own set of reactions, with a means to immediately sound those alarms and frequent drill conducted that will familiarize all personnel with individual responsibilities.

e. Orders and contingency plans must consider recommended actions at various terrorist threat levels and conditions.

f. Contingency plans for major shore commands and their seniors in command exercising territorial authority shall contain provisions for reinforcement of security forces when necessary.

g. Specific matters that are appropriately addressed in most plans include, for example:

(1) Implementation of activity and installation (and regional, if appropriate and feasible) physical security review and assessment programs described in chapter 1.

(2) Protection for vulnerable points/assets within the activity.

(3) Restricted areas and access controls.

(4) Personnel screening/inspection criteria instructions.

(5) Personnel identification and control systems.

(6) Installation of physical security hardware (e.g., intrusion detection systems, barriers, access control systems).

(7) Lock and key control program.

(8) Loss prevention reporting and analyses measures.

(9) Designation of Threat Conditions (THREATCONs) and implementation of associated measures.

(10) Security force organization and training.

(11) Coordination with other security agencies and local law enforcement.

(12) Security response.

(13) Jurisdiction

h. The Physical Security Plan and antiterrorism/force protection (AT/FP) plans (references (g) through (j)) are one and the same provided that they cover crisis management standard operating procedures (i.e., Incident Response Plan), THREATCON implementation plan including a barrier plan (barrier deployment locations, barrier storage locations, and barrier transportation), personnel alerting system, and command center establishment procedures and security.

0202. PLANNING PROCESS

a. Security planning is a continuing process carried out both in advance of operations and concurrently with them.

b. Every asset cannot be made invulnerable. Therefore, the objective of security planning is to identify what assets are to be protected, analyze the threat against them, and develop realistic countermeasures. Increasingly sophisticated methods used by conventional criminals, terrorists, conventional enemy agents, etc., make this an increasingly challenging task. Limited availability of personnel for security duties and money for other security measures exacerbate this challenge. Developing sound security plans to work hand in hand with other related planning (e.g., crisis, force protection, disaster, etc.) requires good decisions by the planning organization based on accurate information, experience, knowledge to orchestrate and integrate security personnel duties such as in-depth protection crime prevention through environmental design to provide in-depth protection.

c. Physical security planning includes the following:

(1) Using electronic security systems to reduce both vulnerability to the threat and reliance on fixed security forces.

(2) Integration of physical security and force protection measures into contingency, mobilization, and wartime plans, and testing of physical security procedures and measures during the exercise of these plans.

(3) Coordinating with installation operations security, crime prevention, information security, personnel security, communications security, automated information security and physical security programs to provide an integrated and coherent effort.

(4) Training security forces at facilities or sites in tactical defense against, and response to, attempted penetrations.

(5) Creating and sustaining physical security awareness.

(6) Identifying resource requirements to apply adequate measures.

0203. PLANNING CONSIDERATIONS. The following factors shall be considered in determination of security requirements and planning:

a. Overall importance/criticality of the command.

(1) Mission and sensitivity of the activity.

(2) Importance of the activity to the continuity of essential naval operations (e.g., combatant support vs. "campus").

b. Force protection.

(1) Terrorist Assessment Plan.

(2) Terrorist Incident Response Plan.

c. Overall susceptibility/vulnerability of the command to threats. Specifically:

(1) The threat to a specific command as defined by military intelligence and investigative agencies.

(2) Ease of access to vital equipment and material.

(3) Location, size, deployment and vulnerability of facilities within the activity and the number of personnel involved.

(4) Need for tailoring security measures to mission critical operating constraints and other local considerations.

(5) Probable duration of operations.

(6) Geographic location (existence of natural barriers).

(7) Legal jurisdiction of real property.

(8) Mutual aid and assistance agreements.

(9) Local political climate.

(10) Adequacy of storage facilities for valuable or sensitive material, including precious metals, drugs, arms, ammunition, and explosives.

(11) Accessibility of the activity to disruptive, criminal, subversive or terrorist elements.

(12) Possible losses and their impact on command mission and readiness.

(13) Possibility or probability of expansion, curtailment or other changes in operations.

(14) Overall cost of security.

(15) Availability of personnel and material.

(16) Coordination of security forces.

(17) Calculated risk.

(18) Potential for increase in threat.

0204. PHYSICAL SECURITY PERFORMANCE GOAL, DOD THREAT MATRIX, AND DOD ASSETS PRIORITIZATION

a. Physical Security System Performance Goal

(1) The goal of the security system for an asset or facility is to deploy security resources to preclude or reduce the potential for sabotage, theft, trespass, terrorism, espionage, or other criminal activity. To achieve this goal, a security system provides the capability to detect, assess, communicate, delay, and respond to an unauthorized attempt at entry.

(2) The components of a security system each have a function and related measures which provide an integrated capability for the following:

(a) Detection, accomplished through human, animal, or electronic means, alerts security personnel to possible threats and attempts at unauthorized entry at or shortly after the time of occurrence;

(b) Assessment, through use of video subsystems, patrols, or fixed posts, assists in localizing and determining the size and intention of an unauthorized intrusion or activity;

(c) Command and control, through diverse and secure communications to ensure that all countermeasures contribute to preventing or containing sabotage, theft, or other criminal activity;

(d) Delay, through the use of active and passive security measures, including barriers, impedes intruders in their efforts to reach their objective;

(e) Response, through the use of designated, trained, and properly equipped security forces. Detection and delay must provide sufficient warning and protection to the asset until the response force can be expected to arrive at the scene.

b. Physical Security Threat Matrix. Figure 2-1 is a description of the DoD generic threat types developed for the physical security program. Using these threat types as a guide, commanders shall develop program, system, command, or installation threat statements which assess potential security threats to critical assets. Using both law enforcement and intelligence information, these assessments should categorize opportunity (when possible) and capabilities of potential adversaries. Physical security threat statements will be used for the development of security systems tailored to the protection of assets and items of security interest.

c. Prioritization of Assets. At figure 2-2 is a description of the DoD resource and asset prioritization scheme with examples of typical assets, a criticality definition, and an example of a typical security system for each level.

0205. THREAT ASSESSMENTS. Additional standards and direction concerning threat assessments are provided in reference (h).

0206. RISK MANAGEMENT. Risk management is the concept which dictates that when there are limited resources available for protection, possible loss or damage to some supplies or to a portion of the activity is risked in order to ensure a greater degree of security to the remaining supplies or portions of the activity. However, security controls shall not be relaxed to the degree that anything is left completely unprotected.

0207. CRISIS SITUATIONS. In evaluating the need for and extent of physical protection required, the possibility of injury to security force personnel must be considered. This is especially relevant when addressing security measures taken during crisis situations (e.g., bomb threats, fires, terrorist incidents or natural catastrophes) to protect government assets; to limit damage and provide emergency services for containment of the incident; and to restore the target activity to normal operation. Situations which present unique and growing physical security problems are: the handling of bomb threats and terrorist incidents as well as any change to higher threat conditions (THREATCONS) (references (g) through (j) pertain). Bomb threat situation planning should be coordinated and cross referenced with the command disaster preparedness plan and integrated with the terrorist incident response plan and should include preventive measures to reduce the opportunities for introduction of bombs; procedures for evaluating and handling

THREAT TYPE	THREAT DESCRIPTION	THREAT EXAMPLE
MAXIMUM	INDIVIDUALS IN ORGANIZED AND TRAINED GROUPS ALONE/WITH ASSISTANCE FROM AN INSIDER; SKILLED, ARMED AND EQUIPPED WITH PENETRATION AIDS	TERRORISTS AND SPECIAL PURPOSE FORCES; HIGHLY TRAINED INTELLIGENCE AGENTS
ADVANCED	INDIVIDUAL(S) WORKING ALONE/IN COLLUSION WITH AN INSIDER; SKILLED OR SEMISKILLED WITHOUT PENETRATION AIDS	HIGHLY ORGANIZED CRIMINAL ELEMENTS; TERRORISTS OR PARAMILITARY FORCES; FOREIGN INTELLIGENCE AGENTS WITH ACCESS
INTERMEDIATE	INDIVIDUAL(S) OR INSIDER(S) WORKING ALONE/IN SMALL GROUPS; SOME KNOWLEDGE OR FAMILIARITY OF SECURITY SYSTEM	CAREER CRIMINALS; ORGANIZED CRIME; WHITE COLLAR CRIMINALS; ACTIVE DEMONSTRATORS; COVERT INTELLIGENCE COLLECTORS; SOME TERRORIST GROUPS
LOW	INDIVIDUAL(S) OR INSIDER(S) WORKING ALONE/IN A SMALL GROUP	CASUAL INTRUDERS; PILFERERS AND THIEVES; OVERT INTELLIGENCE COLLECTORS; PASSIVE DEMONSTRATORS

Figure 2-1. Physical Security Threat Matrix

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
A INTEGRATED ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, ACCESS DELAY AND DENIAL SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED IMMEDIATE RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE WILL RESULT IN GREAT HARM TO THE STRATEGIC CAPABILITY OF THE UNITED STATES	NUCLEAR AND CHEMICAL WEAPONS AND ALERT/MATED DELIVERY SYSTEMS CRITICAL COMMAND, CONTROL AND COMMUNICATIONS FACILITIES AND SYSTEMS CRITICAL INTELLIGENCE GATHERING FACILITIES AND SYSTEMS PRESIDENTIAL TRANSPORT SYSTEMS NUCLEAR REACTORS AND CATEGORY I AND II SPECIAL NUCLEAR MATERIALS RESEARCH, DEVELOPMENT AND TEST ASSETS

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
B ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD BE EXPECTED TO GRAVELY HARM THE OPERATIONAL CAPABILITY OF THE UNITED STATES	ALERT SYSTEMS, FORCES, AND FACILITIES ESSENTIAL COMMAND, CONTROL, AND COMMUNICATIONS FACILITIES AND SYSTEMS CATEGORY I ARMS, AMMUNITION, AND EXPLOSIVES RESEARCH, DEVELOPMENT AND TEST ASSETS

Figure 2-2. Resource and Asset Priorities

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
C ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIERS, SECURITY PATROLS, DESIGNATED RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD IMPACT UPON THE TACTICAL CAPABILITY OF THE UNITED STATES	NONALERT RESOURCES AND ASSETS PRECISION GUIDED MUNITIONS COMMAND, CONTROL, AND COMMUNICATIONS FACILITIES AND SYSTEMS CATEGORY II ARMS, AMMUNITION AND EXPLOSIVE POL/POWER/WATER/SUPPLY STORAGE FACILITIES RESEARCH, DEVELOPMENT AND TEST ASSETS

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
D ELECTRONIC SECURITY SYSTEMS, ACCESS CONTROL, BARRIERS, DESIGNATED RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD COMPROMISE THE DEFENSE INFRASTRUCTURE OF THE UNITED STATES	ARMS, AMMUNITION, AND EXPLOSIVES EXCHANGES AND COMMISSARIES, FUND ACTIVITIES CONTROLLED DRUGS AND PRECIOUS METALS TRAINING ASSETS RESEARCH, DEVELOPMENT AND TEST ASSETS

Figure 2-2 (Contd). Resource and Asset Priorities

threatening messages; policy on evacuation and safety of personnel; procedures for search; procedures for obtaining assistance and support of law enforcement and military explosive ordnance disposal (EOD) units; procedures in the event a bomb is found on the premises; and procedures to be followed in the event of an explosion or detonation.

0208. SABOTAGE. As a minimum measure, assigned personnel should be made aware of the nature of the threat posed by anti-military individuals and groups. Active liaison with the Naval Criminal Investigative Service or command intelligence personnel is a major factor in obtaining such information at the local level.

0209. TERRORISM. Acts of terrorism directed at Navy personnel, activities or installations have the potential to destroy critical facilities, injure or kill personnel, impair or delay accomplishment of mission and cause incalculable damage. Standards and guidance for planning for responding to terrorist acts are contained in references (g) through (j).

0210. THREAT CONDITIONS (THREATCONS) FOR Combating TERRORISM. Requirements and guidelines concerning THREATCONS are outlined in reference (g).

0211. COORDINATION. To provide for efficient coverage of security needs without wasteful duplication:

a. Physical security of separate activities and installations will be coordinated with other military activities/installations in the immediate geographic region or area and with local civilian law enforcement agencies or host government representatives. Opportunities to "partner" or share special capabilities among regional users will be fully explored and documented to ensure economy of effort.

b. Within the physical confines of the installation, the host activity shall coordinate physical security measures employed by tenant activities.

c. The physical security of all arms, ammunition and explosives, and other hazardous material held by tenant activities will be closely coordinated with the host activity.

d. All planning that may result in the physical relocation of an organizational element, physical changes to a facility or a realignment of functions will include the security officer from the outset to ensure that security considerations are included during initial planning.